IJOBSOR, 11 (4) (2024) pp. 493-499

Published by: TRIGIN Publisher

International Journal of Politics and Sociology Research

Journal homepage: www.ijobsor.pelnus.ac.id

Customer protection of digital services by commercial banks concerning consumer and community protection in the financial services sector

Trisadini Prasastinah Usanti[1], Anindya Prastiwi Setiawati[2]

[1]Department of Law, Airlangga University, Surabaya, Indonesia

[2]Department of Economy, Yos Sudarso University, Medan, Indonesia

ARTICLE INFO

Article history:

Received Jan 16, 2024
Revised Feb 09 2024
Accepted Mar 19, 2024

Keywords:

Protection
Consumer
Digital Service

ABSTRACT

In this digital era, banks must adjust themselves, given the needs of customers who want rapidity and flexibility of banking services so that customers can quickly and safely anytime, anywhere. Almost all commercial banks have digital services, but on the other hand, there are potential risks that will be faced. The problems discussed in this study are the potential risks in digital services and risk management related to the protection of customer rights. The approaches used in this research include statutory and conceptual approaches. The result of this research is that the main risks faced in digital services are operational risk, strategic risk, and reputation risk. So preventive efforts by conducting risk management and ensuring information system security and cyber resilience for Consumer Protection. While repressive protection with a handling mechanism for any questions and / or complaints from consumers. It is emphasized in POJK 22/2023 that banks such as PUJK are required to have and implement a mechanism for handling complaints submitted by consumers. Banks are required to provide consumer complaint services whose scope consists of receiving complaints, handling complaints, and resolving complaints.

Corresponding Author:

Trisadini Prasastinah Usanti,
Department of Law,
Airlangga University,
Dharmawangsa Dalam Selatan, Airlangga, Gubeng, Surabaya, East Java 60286, Indonesia.
Email: trisadini@fh.unair.ac.id

1. INTRODUCTION

Banking is one of the financial service actors that has a strategic role in supporting the implementation of development as mandated in Law Number 7 of 1992 concerning Banking which has been amended by Law Number 10 of 1998 (hereinafter referred to as the Banking Law) and amended again with the UU PPSK (Sidik, 2021). This cannot be separated from the two main functions of banks, as intermediary institutions and agents of development. These two functions are interrelated because when the bank performs its function as an intermediary institution it means the bank has carried out its function as an agent of development (Devi & Firmansyah, 2020; Yusuf, Sumarno, & Komarudin, 2022)

As emphasized in the UU PPSK in Article 20 A banks are required to apply prudential principles including risk management in their business activities and banks are required to develop internal procedures regarding the implementation of prudential principles (Disemadi, 2019). The norm in Article 20 A of the UU PPSK is an affirmation norm that has been normed in the Banking Law which requires banks carrying out their business activities to be based on prudential principles.

This cannot be separated from the new era, the digital banking era, which is realized from the beginning of the relationship between the bank and the customer until the relationship ends (Maulidya & Afifah, 2021). It is inevitable that almost all commercial banks have digital services. The existence of digital services provides convenience for customers because it can be accessed anytime and anywhere and minimize direct interaction with bank employees (Haralayya, 2021; Melnychenko, Volosovych, & Baraniuk, 2020; Windasari, Kusumawati, Larasati, & Amelia, 2022), but on the other hand, there are potential risks that will be faced by banks which certainly have an impact on the bank's reputation. So based on the description above, the problems analyzed in this study focus on potential risks in digital services and risk management related to consumer protection (Chairunnisa, Murwadji, & Harrieti, 2024).

Digital services and digital banks have different concepts even though both use information technology. Digital services based on POJK 21/2023 are bank products in the form of services provided by banks utilizing information technology through electronic media to provide access for customers and/or prospective customers regarding Bank products and products and/or services from Bank partners and can be done independently by customers and/or prospective customers (Shanti, Avianto, & Wibowo, 2022). Meanwhile, digital banks based on Financial Services Authority Regulation Number 12 /POJK.03/2021 concerning Commercial Banks (POJK 12/2021) are banks with Indonesian legal entities that provide and carry out business activities mainly through electronic channels without physical offices other than the head office or using limited physical offices. So, if a digital bank is using digital services. However, not all banks that use digital services are digital banks. An example of a digital bank are Bank Jago, Neo Bank, and Allo Bank, while commercial banks in general have used digital services, with types of services in the form of SMS Banking, Phone Banking, Mobile Banking, and Internet Banking (Sitorus, 2023).

Research conducted by Yushita (2008) focuses on risk management arising from bank business activities. Risks in banking business activities must be managed by carrying out risk management. Previous research focused more on risk management efforts in bank business activities and the changing face of banking in digital services that have the potential to suffer losses due to cybercrime and the provisions used are still old regulations, while this study will focus on the risks faced by banks in digital services associated with consumer protection as stipulated in Financial Services Authority Regulation Number 21 of 2023 concerning Digital Services by Commercial Banks and Financial Services Authority Regulation Number 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector, where these regulations have not been discussed in previous studies.

2. RESEARCH METHOD

This research is legal research that involves logic with the skill of building legal arguments as a process of exploring legal science, not just knowing the law (Marzuki, 2016). The approach used is a statutory approach, which is an approach carried out by examining legislation in the form of laws and implementing regulations related to the research topic and a conceptual approach, which examines the concepts of risk, risk management, digital services, and consumer protection. The legal materials used are primary legal materials and secondary legal materials. Primary legal materials include Banking Law, Consumer Protection Law, UU PPSK, and its Implementation Regulations. While secondary legal materials are books, reputable national and international journals, and research reports.

3. RESULTS AND DISCUSSIONS

Risk Management in Digital Services

Business activities carried out by banks are full of risks related to their function as intermediary institutions (Bhegawati & Utama, 2020) With developments in the digital era, the risks faced by banks are increasingly complex so banks are required to implement risk management. Especially in digital services, on the one hand, provide convenience to customers but on the other hand, there is an increase in the risks faced by banks, especially operational risk, strategic risk, and reputation risk. Therefore, in developing digital services, banks must pay attention to aspects of risk management, customer data security, and consumer protection (Gitazia & Muhaimin, 2023).

Referring to the guidelines for the implementation of digital branches by commercial banks, what is meant by digital services is banking services or activities using electronic or digital facilities owned by the Bank, and/or through digital media owned by prospective customers and/or Bank customers, which are carried out independently (Luthfiatussa'dyah, Kosim, & Abristadevi, 2023). This allows prospective customers and/or Bank customers to obtain information, conduct communication, registration, account opening, banking transactions, and account closure, including obtaining other information and transactions outside of banking products, including financial advisory, investment, electronic-based trading system transactions (e-commerce), and other Bank customers' needs (Puspitadewi, 2019).

In the attachment to POJK 21/2023, there is a bank statement that the implementation of digital services must be committed to applying prudential principles and consumer protection principles. Business activities carried out by banks must be based on prudential principles considering that banks are institutions of trust so their existence depends on public trust in banks so banks must maintain public trust (Fitri & Suherman, 2020). One of the manifestations of the prudential principle is the regulation of risk management that must be carried out by banks. Through the implementation of risk management, banks can measure and control the risks faced in their business activities, especially in digital services.

In the implementation of digital services, banks must fulfill several things in the context of implementing information technology risk management, as follows:

a. Logic security, the Bank: Apply the principle of two-factor authentication at the time of registration of prospective customers and at the time of transactions; Use e-KTP as the database and verification of prospective customers; Use an e-KTP reader that has been certified by an authorized institution in accordance with applicable regulations; Storing images of the e-KTP of prospective customers; Storing prospective customer information for the implementation of the APU-PPT program; Validate some prospective customer data against existing population data at Dukcapil; Determine the tolerance limit for data verification input errors; Maintain the confidentiality of personal information of customers or prospective customers during the registration process, transactions, and other services; Ensuring that all devices and applications used in the digital branch have complied with other applicable regulations.
b. Physical security, the Bank: Securing all facilities and infrastructure, such as e-KTP reader machines, terminals, and network cables; Using electronic devices that are tempered proof; Operates Closed-Circuit Television (CCTV) cameras that can cover the entire digital branch area and supporting infrastructure, and stores CCTV camera recordings for a certain period according to Bank policy.
c. Operational control, the Bank: Provides guidelines, explanations, and illustrations of the types and ways of using services at the digital branch as part of the education and customer protection aspects; Verify and ensure the validity and suitability of the mobile phone number registered by the customer, by sending a one-time password (OTP) code to the registered mobile phone number; Provide proof of transaction in electronic or printed form to the customer; Provide notification services to customers for certain types of transactions in accordance with the Bank's risk appetite or customer needs; Have a method of monitoring digital branch activities, including providing an audit trail of the system used in supporting the implementation of the digital branch; Have a mechanism to ensure the security of logs on the e-KTP reader machine; Maintain the security and confidentiality of biometric data, in terms of bank biometric data records of prospective customers; Provide telephone facilities at the digital branch to communicate with the call center; Have functions and procedures to handle customer complaints and dispute resolution related to digital transactions; Have an adequate Disaster Recovery Plan (DRP) to ensure the availability of services at the digital branch; Conducting an audit of the digital branch infrastructure periodically at least one time a year; Ensure that third parties cooperating with the Bank implement adequate security controls at least following the risk appetite and standards owned by the Bank, in terms of services provided by the Bank are the result of cooperation and/or third-party products.

As mentioned earlier, the risks faced by banks in digital services are especially operational risk, strategic risk, and reputation risk, although it does not rule out other risks faced by banks in their business activities, such as credit risk, market risk, liquidity risk, legal risk, and compliance risk. Risk

in the law of engagement has a distinctive meaning. Risk is a principle about who must bear compensation if the debtor does not fulfill his obligations under force majeure (Setiawan, 2021). Meanwhile, risk according to Article 1 point 1 of the Financial Services Authority Regulation Number 18 /POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks (POJK 18/2016) is defined as the potential loss due to the occurrence of certain events.

The risks faced in digital services are operational risks due to inadequate and/or malfunctioning internal processes, human error, system failure, and/or external events that affect the Bank's operations. Meanwhile, strategic risk is caused by the inaccuracy in taking and/or implementing a strategic decision and failure to anticipate changes in the business environment. Lastly, reputation risk is caused by the Bank's failure to comply with and/or non-implementation of laws and regulations.

In research conducted by Cahyolaksono, Mahardhika, & Zakaria (2021) there are several reasons why this risk can arise, the first reason is incomplete regulations regarding bank internal control. OJK as an institution authorized to regulate and supervise financial services institutions does not yet have appropriate regulations governing the internal company employees' control. In addition, OJK will take action on violations committed if there are reports or complaints from victims. OJK only takes action independently on violations that come from secondary data (financial reports, etc.). So, there are still many violations committed by unscrupulous banks. Meanwhile, reputation risk arises due to operational risk. Reputation is obtained from the bank's performance during operation. If there are violations during operation, the bank can lose customer trust. This is because the bank, which is supposed to be a safe solution for saving money, actually becomes an unsafe place to save customers money. Similarly, Yustisia (2022) stated that the provisions regarding the Bank's obligations in organizing digital services which are part of electronic transactions are an effort to maintain the reliability of the digital banking system used.

Customer Rights in Digital Services

There is no specific provision for customer protection in digital services. However, it does not eliminate the rights of customers as consumers who are harmed by digital services to enforce their rights. The provisions used as the basis for protecting customer rights of digital services are the provisions for financial services consumers as stipulated in the Financial Services Authority Regulation Number 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector (POJK 22/2023) (Talumewo, 2013)

It is emphasized in Article 4 of POJK 22/2023 that financial services business actors (PUJK), in this case, one of which is a commercial bank, are required to act in good faith in carrying out their business activities and providing products or services to prospective consumers and consumers. PUJK must treat or serve consumers in a non-discriminatory manner unless otherwise specified in laws regulations or agreements. PUJK must ensure that third parties working to represent the interests of PUJK treat or serve consumers in a non-discriminatory manner. PUJK is prohibited from taking actions that violate the provisions of laws and regulations or norms prevailing in the community which can cause physical and psychological disturbance to prospective consumers or consumers in carrying out business activities. If PUJK violates these provisions, administrative sanctions will be given in the form of: Written warning; Restriction of products and/or services and/or business activities for part or all; Suspension of products and/or services and/or business activities for part or all; Dismissal of the management; Administrative fine; Revocation of product and/or service license; and/or Revocation of business license.

Banks are required to have and implement written consumer protection policies and procedures contained in: Product and/or service design; Provision of product information and/or service; Delivery of product information and/or service; Marketing of products and/or services; Preparation of agreements related to products and/or services; Provision of services for the use of products and/or services; and Handling of complaints and settlement of disputes over products and/or services.

The written procedure fund policy contains equal access to every consumer, special services related to consumers with disabilities and the elderly, protection of consumer assets, protection of

consumer data and/or information, information on handling and resolving complaints from consumers, and mechanisms for using consumer personal data and/or information.

No less important protection for consumers in digital banking services is ensuring the safety and reliability of information systems and cyber resilience, the bank's ability to maintain business continuity by taking anticipatory, adaptive, and proactive actions against cyber threats. PUJK ensures the cyber resilience process is supported by an adequate cyber resilience information system. An adequate cyber resilience information system is an information system that can support the entire process of maintaining cyber resilience, in accordance with the size and complexity of the bank's business.

Article 10 of POJK 22/2023 stipulates that banks as PUJK must be responsible for consumer losses arising from errors, negligence, and/or actions contrary to the provisions of laws and regulations in the financial services sector, committed by the Board of Directors, Board of Commissioners, Employees, and/or third parties working for or representing the interests of PUJK. However, if the PUJK can prove that there was involvement, error, negligence, and/or actions contrary to the provisions of the laws and regulations in the financial services sector committed by the consumer, then the PUJK is not responsible for the consumer losses incurred. The form of responsibility for consumer losses can be agreed upon by consumers and PUJK.

Article 6 POJK 22/2023 also emphasizes that PUJK is also entitled to legal protection from consumers who have bad faith. For example, consumers provide information and/or documents that are unclear, inaccurate, false, and misleading, consumers refuse to carry out obligations as stated in the agreement and use threats or violence, consumers transfer goods that become collateral for credit or financing products without PUJK approval; and consumers submit collateral sourced from criminal acts.

Digital services will not be separated from the presence of standard agreements in electronic form. PUJK must provide access to consumers to obtain and/or print a copy of the standard agreement document. In addition, based on Article 46 POJK 22/2023, PUJK is also prohibited from making and using standard agreements that contain exoneration/exclusion clauses, clauses that state the transfer of PUJK's responsibilities or obligations to consumers. The prohibition of exoneration clauses is also regulated in Article 238 paragraph (4 a) UU PPSK Jo. Article 18 paragraph (1) letter (a) of Law Number 8 Year 1999 on Consumer Protection as a legal protection for consumers in general.

Therefore, legal protection for customer rights as consumers includes preventive protection as previously described (Candrawati, 2014) and repressive protection through a handling mechanism for any questions and/or complaints from customers (Jahri, 2017). Article 68 POJK 22/2023 states that PUJK is obliged to have and implement a mechanism for handling complaints from consumers. PUJK must provide consumer complaint services whose scope consists of: Receipt of complaints; Complaint handling; Complaint resolution.

Complaints filed by consumers must be received, recorded, and documented by the bank. Complaints filed by consumers can be made orally and/or in writing. After receiving the complaint, the bank must handle the complaint in writing with documents consisting of: Consumer identity; Type and date of product and/or service utilization; The problem complaints and Other documents.

The bank as PUJK is obliged to follow up and resolve complaints verbally no later than 5 working days from the time the complaint is received by the bank, while resolving complaints in writing no later than 10 working days from the time the documents are received in full by the bank. A bank may refuse to handle a consumer complaint if: The consumer does not complete the required documents within the stipulated period; The complaint has previously been resolved by the PUJK following this Financial Services Authority Regulation; The complaint is not related to material, reasonable, and direct losses and/or potential losses as stated in the agreement and/or utilization document of the product and/or service; The complaint is not related to the utilization of products and/or services issued by the PUJK concerned; and/or The complaint is in process or has been decided by a civil judicial institution.

If there is no agreement on the handling of complaints made by the bank as PUJK with consumers, they can submit complaints to the OJK for handling complaints in accordance with OJK's authority or submit disputes to the Financial Services Sector Alternative Dispute Resolution

Institution (LAPS) approved by OJK or to the court. If there is a lawsuit for unlawful acts committed by the bank, proving the element of fault is the responsibility of the bank as PUJK, this is emphasized in Article 82 POJK 22/203 Jo. Article 245 UU PPSK.

This was also stated by Tarigan & Paulus (2019 that customer protection for the implementation of digital banking services can be done by preventing or overcoming circumstances that are not expected later by customers through legislation, this protection is known as preventive protection. Then there is protection of customers for unwanted circumstances above that have occurred and harmed customers, so there needs to be an effort to resolve the problem. Protection whose purpose is to resolve problems or disputes that arise is known as repressive protection.

4. CONCLUSION

It is undeniable that in the digital banking era, consumers also have to adapt. Given the needs of customers who want rapidity and flexibility of banking services so that customers can access anytime, anywhere quickly and safely. So that almost all commercial banks have digital services, but on the other hand there are potential risks that will be faced by banks. Legal protection for customer rights as consumers includes preventive protection and repressive protection. Preventive protection by conducting risk management on operational risk, strategic risk, reputation risk, and banks must ensure information system security and cyber resilience for Consumer Protection. While repressive protection with a handling mechanism for any questions and/or complaints from customers. It is emphasized in POJK 22/2023 that banks such as PUJK must have and implement a mechanism for handling complaints submitted by consumers. Banks are required to provide consumer complaint services whose scope consists of receiving complaints, handling complaints, and resolving complaints a statement that what is expected, so there is compatibility. This research techniques used statutory approach by examining legislation that still continuously develop and deserves attention of future research. Moreover, it can also be added the prospect of the development of research method prospects of further studies into the next. Future researchers are expected to examine more deeply the eligibility system of products and / or services in Digital Bank electronic transactions, so that it becomes clearer the Digital Bank security system that causes customer rights not to be properly protected and / or there are still cases of fraud in Digital Bank transaction activities.

ACKNOWLEDGEMENTS

Author would like to acknowledge people who help this research and all supporting from my university

REFERENCES

Bhegawati, D. A. S., & Utama, M. S. (2020). The Role of Banking in Indonesia in Increasing Economic Growth and Community Welfare. *South East Asia Journal of Contemporary Business, Economics and Law*, *22*(1).

Cahyolaksono, B. A., Mahardhika, A., & Zakaria, M. I. (2021). Usulan kebijakan pencegahan risiko perbankan di era digital. *Entrepreneurship Bisnis Manajemen Akuntansi (E-BISMA)*, *2*(1). https://doi.org/https://doi.org/10.37631/e-bisma.v2i1.301

Candrawati, N. N. A. (2014). Perlindungan Hukum terhadap Pemegang Kartu E-money sebagai Alat Pembayaran dalam Transaksi Komersial. *Jurnal Magister Hukum Udayana*, *3*(1), 1–16.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(1), 1–16. https://doi.org/https://doi.org/10.51903/hakim.v2i1.1535

Devi, A., & Firmansyah, I. (2020). Efficiency Determinant Analysis in Islamic Bank in Indonesia. *Journal of Islamic Economics and Banking, MUQTASID*, *11*(2). https://doi.org/https://doi.org/10.18326/muqtasid.v11i2.104-116

Disemadi, H. S. (2019). Risk Management In The Provision of People's Business Credit as Implementation of Prudential Principles. *Diponegoro Law Review*, *4*(2), 194–208. https://doi.org/https://doi.org/10.14710/dilrev.4.2.2019.194-208

Fitri, D., & Suherman. (2020). Perlindungan Hukum Terhadap Nasabah Perbankan Yang Mengalami Kerugian Atas Pembobolan Rekening. *2ndNational ConferenceonLaw Studies: Legal Development Towards A Digital Society Era*, *2*(1).

Gitazia, A. R., & Muhaimin. (2023). Tinjauan Yuridis Bank Digital Dalam Perspektif Bank Indonesia. *Jurnal Commerce Law*, *3*(1).

Haralayya, B. (2021). How Digital Banking has Brought Innovative Products and Services to India. *Journal of Advanced Research in Quality Control & Management*, *6*(1), 15–17.

Jahri, A. (2017). Perlindungan Nasabah Debitur Terhadap Perjanjian Baku Yang Mengandung Klausula Eksonerasi Pada Bank Umum Di Bandarlampung. *Fiat Justisia: Jurnal Ilmu Hukum*, *10*(1). https://doi.org/https://doi.org/10.25041/fiatjustisia.v10no1.651

Luthfiatussa'dyah, D., Kosim, A. M., & Abristadevi. (2023). Strategi Optimalisasi Digitalisasi Produk Perbankan pada Bank Syariah Indonesia. *Jurnal Kajian Ekonomi & Bisnis Islam, El-Mal*, *4*(3). https://doi.org/1047467/elmal.v4i3.2073

Marzuki, P. M. (2016). *Penelitian Hukum* (Edisi Revi). Jakarta: Kencana Perdana Media Group.

Maulidya, G. P., & Afifah, N. (2021). Perbankan Dalam Era Baru Digital : Menuju Bank 4.0. *Proceeding Seminar Bisnis Seri V*.

Melnychenko, S., Volosovych, S., & Baraniuk, Y. (2020). Dominant Ideas Of Financial Technologies In Digital Banking. *Baltic Journal of Economic Studies*, *6*(1). https://doi.org/10.30525/2256-0742/2020-6-1-92-99

Puspitadewi, I. (2019). Pengaruh Digitalisasi Perbankan Terhadap Efektivitas Dan Produktivitas Kerja Pegawai. *Jurnal Manajemen Dan Bisnis Indonesia*, *5*(2), 247–258.

Setiawan, I. K. O. (2021). *Hukum Perikatan*. Jakarta: Bumi Aksara.

Shanti, R., Avianto, W., & Wibowo, W. A. (2022). A Systematic Review on Banking Digital Transformation. *Jurnal Administrare: Jurnal Pemikiran Ilmiah Dan Pendidikan Administrasi Perkantoran*, *9*(2).

Sidik, A. P. P. (2021). Role Of Law In Banking For National Economic Development. *Webology*, *18*(6).

Sitorus, H. A. M. (2023). Perlindungan Hukum Terhadap Nasabah Atas Fraud Pada Transaksi Bank Digital. *Jurnal Ilmu Sosial Dan Pendidikan (JISIP)*, *7*(1). https://doi.org/10.58258/jisip.v7i1.4428/http://ejournal.mandalanursa.org/index.php/JISIP/index

Talumewo, F. (2013). Pertanggungjawaban Bank Terhadap Nasabah Yang Menjadi Korban Kejahatan Informasi dan Transaksi Elektronik (ITE). *LEX CRIMEN*, *2*(1).

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia, 1*(3), 294–307. https://doi.org/https://doi.org/10.14710/jphi.v1i3.294-307

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge (JIK)*, *7*(2), 1–10. https://doi.org/https://doi.org/10.1016/j.jik.2022.100170

Yushita, A. N. (2008). Implementasi risk management pada industri perbankan nasional. *Jurnal Pendidikan Akuntansi Indonesia*, *6*(1). https://doi.org/https://doi.org/10.21831/jpai.v6i1.1792

Yustisia, M. P. (2022). Perlindungan Bagi Nasabah Dalam Penyelenggaraan Layanan Perbankan Digital di Indonesia. *Dharmasisya (Jurnal Program Magister Hukum FHUI)*, *2*(20).

Yusuf, M., Sumarno, & Komarudin, P. (2022). Bank Digital Syariah di Indonesia: Telaah Regulasi Dan Perlindungan Nasabah. *Al-Infaq: Jurnal Ekonomi Islam*, *13*(2).

.